

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division**

UNITED STATES OF AMERICA

v.

GERALD A. DARBY

)
)
)
)
)

Criminal No. 2:16cr36

DEFENDANT’S FIRST MOTION TO SUPPRESS

Gerald A. Darby, through counsel and pursuant to Federal Rule of Criminal Procedure 12(b)(3)(c), respectfully moves this Court for an order suppressing all evidence seized from Mr. Darby’s home computer by the FBI on or about January 7, 2016 through the use of a network investigative technique, as well as all fruits of that search. An evidentiary hearing is requested.

INTRODUCTION

On or about January 7, 2016 , the FBI seized evidence from Mr. Darby’s home computer with a “network investigative technique” (NIT), a type of malware that was secretly inserted by FBI agents onto Mr. Darby’s home computer. The evidence seized consisted of an “internet protocol” (IP) address and other electronic data.

The NIT altered and overrode security settings on the computer, allowed the FBI to remotely search for and collect data from the computer’s hard drive, and then transmitted that data to the FBI. Mr. Darby also seeks suppression of all fruits of this illegal search, including any allegedly inculpatory statements by him and any data recovered from Mr. Darby’s computer after its physical seizure pursuant to a second search warrant for Mr. Darby’s home, the probable cause for which was established through the NIT operation.

While the search and seizure technology involved in this case is sophisticated, the key facts are likely to be undisputed and the applicable legal principles are well established. Mr. Darby raises three specific grounds for suppression.

First, the remote search of Mr. Darby's home computer was undertaken pursuant to a warrant that is not supported by probable cause. As set forth below, the Government sought authorization to search the computers of everyone who visited the home (or "log in") page¹ of a web site called "Playpen." See exhs. A and B (the NIT warrant and supporting application).² Probable cause for these searches turned on whether it "unabashedly announced" that it was a child pornography site. Playpen had a mix of legal and illegal content, as well as chat and message forums, and it did not advertise itself as a child pornography site. See ex. C (Playpen's home page).

The lack of facts in support of probable cause is made even more problematic because the Government apparently interpreted the NIT warrant as authorizing 100,000 or more searches anywhere in the world. As a result, the scope of the search and seizure authority allegedly authorized by this warrant is unprecedented.

Second, the FBI intentionally or recklessly misled the issuing court about how the site appeared, among other false and misleading statements. Specifically, the warrant application alleged that the site's home page displayed purportedly lascivious pictures that advertised illegal content on the site. In truth, the FBI had seized control of the site before applying for the

¹ The homepage is also referred to as the "main page" in the affidavit submitted in support of the NIT warrant. The terms "homepage," "main page," or "log in" screen all refer to the screen that was displayed by the website before a visitor "logged in." See ex. C (Playpen's home page).

² The NIT warrant affidavit refers to "TARGET WEBSITE." The affidavit in support of the search warrant authorizing the traditional residential search of Mr. Darby's home in Newport News refers to "Website A." Undersigned counsel believes that these terms both refer to the Tor site called "Playpen."

warrant and knew that these pictures had been removed. The defense therefore requests a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

Third, the NIT warrant was an anticipatory warrant and the “triggering event” that would establish probable cause for searches did not occur. As set forth in the warrant application, the triggering event was the act of visiting Playpen’s home page *as it was described in the application* and then electing to enter the site. However, the triggering event did not occur in this case because the FBI had included a false description of the home page in the application. The home page as it actually appeared at the time the warrant was issued and the searches were executed did not, as the FBI had claimed, show that the site contained child pornography. The search in this case therefore exceeded the scope of the warrant’s authorization and suppression is required.

In short, this case presents novel and important issues involving the Fourth Amendment and privacy rights in an increasingly Internet-driven world, governmental adherence to the rule of law, and the Government’s duty of candor to the courts. Any one of the grounds set forth in this motion warrants suppression. When the Court considers the totality of the circumstances, suppression is not only appropriate but necessary to deter future overreaching by the Government.

STATEMENT OF FACTS

A. The Playpen Web Site and the Tor Network

On January 7, 2016, law enforcement agents executed a search warrant at the home of Gerald A. Darby in Suffolk, Virginia, and physically seized (among other items) several personal computers. This search occurred when the FBI used a “Network Investigative Technique” (NIT) malware to conduct a remote search of the contents of Mr. Darby’s personal computer. It is this data search that is the focus of Mr. Darby’s Fourth Amendment challenge here.

According to the discovery, the events leading to the search of Mr. Darby’s home began in December, 2014, when a “foreign law enforcement agency” happened upon the website Playpen, learned that it contained child pornography, and alerted the FBI. Ex. B (NIT warrant application) at ¶ 28.

Playpen operated on a network commonly known as “the onion router” or “Tor” network. Tor was created by the U.S. Naval Research Laboratory and it is primarily funded by the U.S. Government. When operating as designed, the network “protects users’ privacy online.” Ex. B at ¶ 8. In simple terms, people who want to use the Tor network can download a free browser and search engine (similar to Chrome or other Internet browsers) that provides added privacy protections. See <https://www.torproject.org> (“Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security”). Activities and communications on Tor (like visiting a website) are routed through multiple computers (or “nodes”) to protect the confidentiality of the Internet Protocol (IP) addresses and

other identifying information of its users. *See* ex. B at ¶¶ 6-9. Using the Tor network is comparable to having the Internet equivalent of an unlisted phone number and caller I.D. blocking.

Like the Internet in general, the Tor network can be used for both legitimate and illicit purposes. *See* James Ball, *Guardian Launches Secure Drop System for Whistleblowers to Share Files*, *The Guardian*, June 5, 2014 (describing the newspaper's use of Tor as a secure means for communicating with whistleblowers);³ Virginia Heffernan, *Granting Anonymity*, *N.Y. Times*, December 17, 2010 ("Peaceniks and human rights groups use Tor, as do journalists, private citizens and the military, and the heterogeneity and farflungness of its users – together with its elegant source code – keep it unbreachable.").⁴ Millions of people now routinely use the Tor network to avoid being targeted by advertising, to protect their personal data from marketing companies and scammers, and to search for a wide variety of content that they wish to keep private.

In this case, due to an error in Playpen's connections with the Tor network, it could be found and viewed on both the Tor network and the regular Internet for at least part of the time that it was operating.⁵ The FBI was able to locate the operator of the site and raided his home in Naples, Florida, on February 19, 2015. *See* ex. B at ¶ 30.

B. The FBI's Distribution of Pornography From Playpen

³ Available at <http://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents> (last accessed Mar. 16, 2016).

⁴ Available at <http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html? r=0> (last accessed Mar. 16, 2016).

⁵ *See* Residential warrant – Bates 0176, ¶ 46 n.5 ("Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional internet.").

The same day, the FBI took control of Playpen and moved its server to a government facility in Virginia, where it maintained and operated the site at least until March 4, 2015.⁶ During this time the FBI continued to operate the site as an active distributor of child pornography and took no measures to block or limit the uploading, downloading or redistribution of thousands of illicit pictures and videos.

As of February 20, the site had 158,094 members from all over the world. Ex. B at ¶ 11. It appears that approximately 56,000 new members joined the site after the FBI took it over and approximately 100,000 people visited the site during the two week period that the FBI was operating it. This was a dramatic increase over the approximately 11,000 weekly visitors the site had before the FBI took it over. *See* Ex. B at ¶ 19.

C. The Virginia “Network Investigative Technique” Warrant

On February 20, 2015, the Government submitted its application for the NIT warrant to Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. In the application, the affiant states that “the entirety of the TARGET WEBSITE is dedicated to child pornography,” ex. B. at ¶ 27, and also describes the site as a “website whose primary purpose is the advertisement and distribution of child pornography.” Ex. B at ¶ 11. More accurately, Playpen offered a mix of chat forums, private messaging services, both legal and illegal pictures and videos, and links to pictures and videos.⁷

⁶ A “server” is basically a computer that stores data for other computers, connects individual computers to Internet networks, and runs various programs that allows web sites to connect to the Internet. *See* ex. B at ¶ 5(e); <http://techterms.com/definition/server>.

⁷The FBI also obtained a separate authorization pursuant to 18 U.S.C. § 2518 (commonly referred to as “Title III” or “the Wiretap Act”) to intercept electronic communications on Playpen’s private chat and messaging services between unknown “target subjects” or “unidentified administrators and users.” This authorization was apparently sought because 18 U.S.C. § 2511 generally prohibits electronic communication service providers from monitoring communication that

The warrant application sought authorization to use a “Network Investigative Technique” to search “activating computers,” which were defined as the computers “of any user or administrator who logs into the TARGET WEBSITE by entering a username or password.” Ex. A at Bates 004 (“Attachment A”). The username and password could be made up and entered on the spot (there was no verification or other steps required to enter the site), and the site was free.

Somewhat confusingly, the actual targets of the NIT warrant were the “activating computers,” not the “TARGET WEBSITE,” which refers to Playpen. Not only had the FBI already seized Playpen, its server and records did not contain the visitor data the FBI wanted to search for pursuant to the NIT warrant. Nor could that data be collected from third parties, such as Comcast or other Internet service providers, since the basic purpose of the Tor browser and network is to privatize its users identities and activities. Ex. B at ¶¶ 8-9, 29.

Accordingly, the warrant application explains that the FBI would use its NIT to search for data directly on the personal computers and other digital devices of anyone who visited the Playpen site. This data included user IP addresses; the type of operating systems on their computers; and various other data that would not otherwise be disclosed by a computer’s owner or user. Ex. A at Bates 005 (“Attachment B”). Elsewhere in the application, the NIT is broadly described as hidden “computer instructions,” or code, that agents would send to the unidentified targets when they landed on the home page and typed in a name or password. Ex. B at ¶ 33. Since this code was “hidden” visitors to the site had no knowledge that their computers were infected with it when they visited Playpen. In sum, the NIT is malware that gained the Government access to personal computers without the owner or user’s knowledge or consent.

take place on their services, and the FBI became the service provider for Playpen’s communication services after February 19, 2015.

Once the FBI had inserted a NIT onto a computer, it did several things to execute a search on and seize data from that computer. First, the NIT altered or overrode a computer's security settings to install itself on the targeted computer, similar to disabling a home's burglar alarm system before climbing through a window.

Next, the NIT searched the computer's hard drive and operating system for the data that the FBI wanted. This is the technical equivalent of searching desks or file cabinets in the house to find an address book or billing records that contain the information the FBI was looking for. In this case, Mr. Darby's computer was located in his home when it was remotely searched by the FBI and he had no knowledge that the search had even occurred until long after the fact.

Finally, the NIT overrode the user's Tor browser protections and forced the computer to send the seized data back to the FBI, where it was stored in the digital equivalent of an evidence room on a government server.

It appears that as many as 100,000 people visited Playpen while it was under FBI control. In related litigation, the Government has maintained that all of those visitors were authorized targets of the NIT searches, and it is unclear at this point how many of the 100,000 potential targets were actually subjected to data searches.

Playpen had a mix of legal and illegal content, as well as chat forums, and the NIT warrant application does not allege that everyone who visited the site necessarily viewed illegal pictures. The warrant application nevertheless sought authorization to search the computers of anyone who simply passed through the home page. The affiant therefore focused on the appearance and contents of the home page to establish probable cause to believe that anyone accessing the site was committing a crime. In this regard, the application describes the home page as containing a banner with "two images depicting partially clothed prepubescent girls with

their legs spread apart.” Ex. B at ¶ 12. The application did not claim that these pictures meet the legal definition of “lascivious” pornography, in 18 U.S.C. § 2256(2)(A), and the application did not include a copy of the home page.

Moreover, the description of the home page was inaccurate.⁸ The home page, as it actually appeared from February 19 (the day before the warrant application) until the site was shut down, is devoid of any highly sexualized images of prepubescent girls, and instead shows a picture of a fully clothed female, legs crossed. While the girl depicted on the home page appears to be young, the image is small and it is not clear that she is under the age of 18, let alone “prepubescent.”

Further, the FBI agents who conducted the February 19 search of the original site operator’s Florida home have confirmed that they clearly would have seen the website when executing that search and thus would have seen the new homepage. Nevertheless, the FBI did not disclose this information in the warrant application presented to Magistrate Judge Buchanan the following day, and it never submitted an amended or corrected affidavit.

The warrant application goes on to describe text on the home page that advises visitors not to “copy and paste” and states “No Cross-Board Posts, .7Z preferred, Encrypt File Names, Include Preview,” along with a place to login or register as a new user. *See* ex. B at ¶ 12. The affiant did not claim that the technical text is indicative of criminality and explained, *inter alia*, that terms like “‘no cross-board reposts’ refers to a rule against posting material that had been posted on other websites. *Id.*

⁸ On March 15, 2016, the defense requested additional discovery related to changes made to the Playpen site and the Government’s knowledge of those changes at various times. At the time of filing (on the deadline for filing all pretrial motions) that discovery request is still outstanding. Accordingly, the defense’s representations and factual recitations are based, in large part, on information that was gained from sources other than the discovery provided thus far in this case. As the United States continues to provide discovery, the defense reserves the right to supplement the facts contained herein.

The rest of the material about the site describes child pornography that could be found in various sub-directories. After signing in to Playpen, visitors were directed to a “table of contents” listing 46 different forums and sub-directories. Like the home page, the table of contents did not contain child pornography (the graphics on the page depict onions, a visual reference to the Tor network) and it listed a variety of topics. Most of these clearly relate to sexual matters or fetishes, and some of these also clearly relate to children. Other than the reference to “HC” (according to the affiant, standing for “hard core”) on four of the forums, it is not obvious that they contain child pornography. Some of the content consisted of written “stories,” legal child “erotica,” and a variety of other forums with names like “general discussion” and “artwork.” *See* ex. B at ¶¶ 5(b) & 14.

The table of contents, moreover, could be viewed only *after* someone had logged in to the site, at which point the FBI had already remotely searched the visitor’s computer. From there, in order to locate pictures or videos, a visitor would have to take the additional steps of selecting one of the sub-directories with a suggestive title; “click on” or open the sub-directory; and then scroll through its content to view what was actually displayed there. Intentionally downloading or copying any of the pictures or videos on view would require additional steps.

D. The Search of Mr. Darby’s Home Computer

The FBI began searching computers on February 20, the same day the NIT warrant was granted. On or about February 27, 2015, FBI agents sent the NIT malware to a computer connected to someone with the username “Broden” and then seized data from it.

On March 4, 2015, the FBI used some of the data it had surreptitiously collected from Mr. Darby’s home computer to prepare an administrative subpoena to Verizon for address

information related to that seized data. Verizon responded with the subscriber information, name, and address associated with Mr. Darby's computer.

On January 7, 2016, FBI and other law enforcement agents searched Mr. Darby's home pursuant to a second warrant issued by the Hon. Robert Krask on January 4, 2016. Pursuant to that warrant agents seized several computers, hard drives, cellular phones, tablets, video game systems, and other personal property.

Mr. Darby has never been previously charged with any kind of criminal offense and there is no allegation that the instant possession charges are related to any "hands-on" or production offenses.

LAW & ARGUMENT

A. The NIT Warrant Was Not Supported by Probable Cause

The NIT warrant authorized the FBI to search the computers of any and all visitors to Playpen from the moment they entered a name or password on the home page. *See* ex. B at ¶ 32 (seeking authority "to investigate any user or administrator *who logs into* the TARGET WEBSITE by entering a user name and password") (emphasis added). The user name and password could be made up and entered on the spot, and the site did not charge any fees. Nor did it verify user information or otherwise require affirmative steps to access the site.

Because there was no particularized information in the warrant application about site visitors and it did not include an expert "collector profile," probable cause for the computer searches turned on the contents of the home (or "log in") page and whether it was likely that anyone who saw that page would know that its contents were illegal before proceeding to actually take a look at the contents. *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2005). While the warrant application asserted that Playpen "advertised" that it was "dedicated"

to child pornography, even a cursory review of its home page shows that this is not correct. *See* ex. C.

Setting aside for the moment the inaccuracy of the warrant application, and taking it at face value, the only facts that would support the conclusion that the site was obviously dedicated to child pornography are the description of two pictures that appear on the site's banner, "located to either side of the site name," "depicting partially clothed prepubescent females with their legs spread apart." Ex. B at ¶ 12.

The affiant did not claim that these pictures met the definition of illegal "lascivious" images, and in fact they do not. *See generally United States v. Doyle*, 650 F.3d 460, 473 (4th Cir. 2011) (noting that the "mere presence of nudity in a photograph, even child nudity, does not constitute child pornography"); *United States v. Battershell*, 457 F.3d 1048, 1051 (9th Cir. 2006) (photograph described as "a young female (8–10 YOA) naked in a bathtub" is "insufficient to establish probable cause that the photograph lasciviously exhibited the genitals or pubic area"); *United States v. Brunette*, 256 F.3d 14, 17 (1st Cir. 2001) (statement that images showed "'a prepubescent boy lasciviously displaying his genitals'" was a "bare legal assertion, absent any descriptive support and without an independent review of the images, [which] was insufficient to sustain . . . probable cause"). Nor did the affiant include a copy of the home page with the warrant application so that Magistrate Judge Buchanan could assess it for herself.

As a result, the affidavit – even if it had been accurate – did not establish probable cause to search the computers of the tens of thousands of people who visited Playpen. This is demonstrated no more clearly than by comparing the homepage (Ex. C) with media pictures of child models and pageant contestants that appear in response to a Google search for "child models." And, without any pictures that are at least arguably "lascivious," there is nothing to

show that Playpen advertised or promoted itself as a child pornography site. In this regard, the rest of the facts in the affidavit about the site relates to general (and frequently erroneous) information about the Tor network; a recitation of some technical text on the home page; and the site's contents. While the last is certainly relevant, it adds little or nothing to the probable cause analysis in this particular case because the Government chose to seek authorization to execute its searches *before* visitors entered the site and could see what it actually contained. *Compare Gourde*, 440 F.3d at 1070 (affidavit established that the defendant had paid for a multi-month membership after having had an opportunity to view samples of the child pornography offered on the site).

In short, given the facts alleged in the affidavit, there can be no reasonable dispute that the critical information for probable cause purposes was the claim that the site displayed “partially clothed prepubescent females with their legs spread apart” and the suggestion, at least, that these images were “lascivious” and illegal. Ex. B at ¶ 12.

The law is clear, however, that when a computer search is based on someone's mere accessing of a website, there is probable cause for a search only if the site's illegal purpose or content is readily apparent. In *Gourde*, the Ninth Circuit carefully considered whether there was probable cause to search the computer of someone based on their membership in a site that distributed child pornography. The question of probable cause turned on how the site would appear to even a first time or casual visitor, and what *Gourde* had done apart from merely visiting the site that manifested his intent to view and possess child pornography. Unlike here, the site in *Gourde* was quite explicit about what it offered.

First, the name of the site was “Lolitagurls.com,” and the term “Lolita” is particularly associated with a prurient focus on young girls. *See United States v. Gourde*, 382 F.3d 1003,

1014 (9th Cir. 2004) (Gould, J. concurring in original panel decision); *see also United States v. Shields*, 458 F.3d 269, 279 (3d Cir. 2006) (warrant affidavit “explained that ‘[s]ometimes individuals whose sexual objects are minors will refer to these images as ‘Lolitas,’ a term whose etymology ‘comes from the titles of old child pornography magazines.’”).

Here, by contrast, the affiant did not allege that the site’s name had any connection to child pornography. To the contrary, the name “Playpen” is widely associated with a “men’s lifestyle” magazine that is a knock-off of Playboy (*see ex. D*); numerous strip clubs around the country, including one that advertises itself as “the premier adult entertainment strip club close to downtown Los Angeles” (*id.*); and popular, legal web sites (such as “Angel’s Playpen” and “Xtreme Playpen”) that feature far more explicit (and entirely legal) pictures of young women than appear on the site at issue here. *Compare ex. C with ex. D.*

Further, unlike Playpen’s home page, the Lolitagurls.com home page brazenly advertised the number and quality of its “Lolita pics,” including “[o]ver one thousand pictures of girls age 12-17! Naked lolita girls with weekly updates! What you will find here at Lolitagurls.com is a complete collection of young girl pics.” 440 F.3d at 1067. Hence, in stark contrast to Playpen, the site in *Gourde*, like that in *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005) (cited in *Gourde*, 440 F.3d at 1072 as involving “nearly identical facts”), “unabashedly announced that its essential purpose was to trade child pornography.” *See also, e.g., Shields*, 458 F.3d at 278 (agreeing with *Martin*’s characterization of site as one that ““unabashedly announced that its essential purpose was to trade child pornography”); *United States v. Froman*, 355 F.3d 882, 890 (5th Cir. 2004) (similar conclusions for same “Candyman” site).⁹

⁹ In *United States v. Ramsburg*, 114 F. App’x 78, 81 (4th Cir. 2004), the Fourth Circuit declined to reach the question whether mere membership in a predominantly illicit organization that also provided unobjectionable services like a “chat” function could support probable cause. Instead the Fourth Circuit relied on separate statements in an amended warrant affidavit alleging that an

Significantly, the site in *Gourde* also charged a membership fee and visitors saw “images of nude and partially-dressed girls, some prepubescent” *before* they paid the fee and joined the site. 440 F.3d at 1067. Unlike with Playpen, which was free and immediately accessible, the court found that Gourde had demonstrated his intent to view and download child pornography because, *after* having viewed samples of the illicit pictures offered on the site, he took the additional “affirmative steps” of entering his credit card information, paying a monthly fee, and maintaining his membership for at least two months. *See id.* at 1071 (“The affidavit left little doubt that Gourde had paid to obtain unlimited access to images of child pornography knowingly and willingly, and not involuntary[il]y, unwittingly, or even passively”).

Given these facts, the court found that the warrant application in *Gourde* had demonstrated that he was not an “accidental browser” or “someone who took advantage of the free tour” offered by the site, but who, after viewing the contents, “balked at taking the active steps necessary to become a member.” *Id.* at 1070. By contrast here, the NIT warrant did nothing to distinguish between “accidental browsers” (or even people looking for legal pornography or more extreme, but still legal, fetish content) and people who, like Gourde, had indisputably viewed samples of the child pornography on offer and then chose not only to join the site, but pay for a continuing membership.

In this regard, the NIT warrant application does not allege that logging into Playpen required any significant steps, like first getting a tour of the site and then paying a membership fee. It does, however, claim that “numerous affirmative steps” were required for users to locate Playpen on the Internet, and therefore it was “extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content.” Ex. B at ¶ 10. Anyone who has even a passing familiarity with the Tor network (or access to Google) would know that these email address linked to the defendant had “transmitted an image of child pornography.” *Id.*

statements are basically nonsense (and will be addressed in further detail below in connection with Mr. Darby's request for *Franks* hearing). In fact, the discovery shows that Playpen came to the attention of law enforcement in the first place because investigators "stumbled upon it" when the site was accessible on both the regular Internet and Tor network.

Moreover, contrary to the affiant's claim that sites cannot be found on the Tor network with the equivalent of a "Google" search (ex. B at ¶ 10), the Tor browser looks like a regular browser and there are a variety of Tor search engines.¹⁰ All a user need do is enter search terms for sexually oriented sites, chat rooms, or a host of other content not related to child pornography to find sites like Playpen. *See, e.g.,* <https://ahmia.fi/search> (search engine that allows use of search terms to find sites on Tor network).

The application also falsely claimed that "Tor hidden services are not indexed like web sites on the traditional Internet." Ex. B at ¶ 10. In fact, the Tor network offers numerous "indexes," which contain links to all sorts of sites with sexual content that may or may not be legal. *See, e.g.,* <http://thehiddenwiki.org/> (the most popular Tor index, which also lists (contrary to the affiant's claims) a variety of Tor search engines).

Finally, the court in *Gourde* relied in part on the fact that the warrant application contained a detailed collector profile that linked Gourde's activities on the site to behavior typically associated with child pornography collectors. 440 F.3d at 1072. Here, by contrast, the warrant application made no attempt to link the act of simply visiting Playpen's home page to specific offender characteristics. As a result, the warrant made no distinction between, on the one hand, casual or "unwitting" visitors and "accidental browsers" and, on the other, the subset of people actively seeking child pornography; here, *both* groups were authorized targets of the

¹⁰ *See* <https://www.torproject.org/projects/torbrowser.html.en> (last accessed Mar. 17, 2016).

FBI's searches. See *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1176 (CDT) (9th Cir. 2010) ("WrongMatishrs and their collaborators have obvious incentives to make data difficult to find, but parties involved in lawful activities may also encrypt or compress data for entirely legitimate reasons: protection of privacy, preservation of privileged communications, warding off industrial espionage or preventing general mischief such as identity theft.").

In short, the probable cause boundaries laid out in *Gourde*, *Martin* and elsewhere make sense, because the Internet is awash with websites that cater to every imaginable taste and fetish, much of which may be utterly repugnant, but is nonetheless legal and even constitutionally protected. See *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 245 (2002) (it is "well established that speech may not be prohibited because it concerns subjects offending our sensibilities"); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 355 (1995) (the right to anonymity while engaging in speech related activities – such as using Tor and Playpen's chat and messaging services – "is an aspect of free speech protected by the First Amendment").

As the Second Circuit recently concluded when reversing the conviction of a police officer charged with planning to attack and cannibalize women, "Although it is increasingly challenging to identify that line [between fantasy and intent] in the Internet age, it still exists and it must be rationally discernible in order to ensure that 'a person's inclinations and fantasies are his own and beyond the reach of the government.'" *United States v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015) (reversing conviction of defendant known as "Girlmeat Hunter" who engaged in gruesome exchanges on fetish websites) (citation omitted). The court went on to emphasize that "[w]e are loath to give the government the power to punish us for our thoughts and not our actions. That includes the power to criminalize an individual's expression of sexual fantasies, no matter how perverse or disturbing." *Id.* (citation omitted).

Although application of probable cause inquiries to websites is similar to the *Gourde* line of cases, the actual facts alleged here are more similar to those presented in *United States v. Doyle*, 650 F.3d 460, 470 (4th Cir. 2011). In *Doyle*, the Fourth Circuit suppressed all evidence from a search for child pornography and found that the good faith exception did not apply “because the affidavit offered in support of the warrant lacked the necessary information from which the issuing magistrate, or executing police officer, could glean probable cause to support a search.” *Id.* In that case, “the only mention in the warrant application regarding the presence of pornography was the statement that one of the alleged victims ‘disclosed to an Uncle that Doyle had shown the victim pictures of nude children.’” *Id.* at 472. Doyle argued that “there was no evidence that the pictures referenced ... [in the affidavit] actually constituted child pornography.” *Id.* at 473. The Fourth Circuit agreed:

The mere presence of nudity in a photograph, even child nudity, does not constitute child pornography as that term is defined by Virginia law. Instead, the picture must contain a “lewd exhibition” of nudity.... [N]othing in the affidavit supports a belief that the alleged pictures showed a “lewd exhibition of nudity” in violation of the Virginia statute. The affidavit therefore lacked probable cause to justify a search of Doyle’s home for child pornography.

Id. (internal citations and quotations omitted). At least in *Doyle*, the affidavit alleged that the depicted children were nude. Here, the affidavit claimed that the homepage of the Playpen site depicted two girls who were “partially clothed.” Ex. B at ¶ 12.

With these principles in mind, even accepting its accuracy for the sake of argument, the NIT warrant application was a very slim reed on which to hang a sweeping authorization to search 100,000 or more computers. Simply put, the NIT warrant was not supported by probable cause.

B. The Court Should Hold a *Franks* Hearing Because the NIT Affidavit Contains, at a Minimum, Recklessly Misleading Statements and Omissions.

The argument above accepts the facts alleged in the warrant application at face value. But the affidavit cannot be taken at face value because several critical allegations were false or misleading. In *Franks v. Delaware*, 438 U.S. 154, 156 (1978), the Supreme Court held that “where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s request.”

The doctrine applies to omissions, not just false statements. *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990); *see also United States v. Eccleston*, 615 F. App’x 767, 780 (4th Cir. 2015). *Franks* relief may also be justified when the “agents’ failure to verify readily available information amount[s] to a reckless disregard for the truth.” *In re Search Warrants Served on Home Health & Hospice Care, Inc.*, 121 F.3d 700 (4th Cir. 1997) (unpublished). And the doctrine further applies when the affiant intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading. *See United States v. Tate*, 524 F.3d 449, 456-57 (4th Cir. 2008). If an omission or statement is recklessly or intentionally false or misleading the court must determine if the offending inaccuracy is “material” to the probable cause determination. “To determine materiality, a court must excise the offending inaccuracies and insert the facts recklessly omitted, and then determine whether or not the ‘corrected’ warrant affidavit would establish probable cause.” *Miller v. Prince George’s Cty.*, 475 F.3d 621, 628 (4th Cir. 2007) (internal quotation marks omitted).

In this case, the false and omitted statements were plainly material. *The description of the home page was a pivotal component of the affiant’s allegations in support of probable*

cause. The affiant's burden, after all, was not just to show that Playpen contained child pornography. If that is all that were required, then someone could have his home searched simply for entering a bookstore that sold child pornography from under the counter, even though all he was looking for was a copy of Playboy. *Cf. Ramsburg*, 114 F. App'x at 81 (declining to hold that mere membership in a predominantly illicit online organization gives probable cause to support search).

Instead, in order to support a sweeping authorization to search the computers of anyone who accessed the site, the Government aimed to persuade the Magistrate Judge that the site was not only "dedicated" to child pornography, but that this purpose would be apparent to anyone who viewed its public home page and therefore would know what he or she was getting into. The affidavit accomplished that (if it did so at all) by including a patently inaccurate description of the homepage in the supporting affidavit, despite the fact that the FBI knew (or clearly should have known) before applying for the warrant that it was inaccurate. These facts alone warrant a *Franks* hearing. To make matters worse, the false description of the home page was accompanied by other lesser but nonetheless false statements and omissions that, taken as a whole, resulted in a highly confusing and misleading affidavit.

To begin, the affiant claimed that "the entirety of the TARGET WEBSITE is dedicated to child pornography." Ex. B at ¶ 27. As noted above, the content of the site is not a critical part of the probable cause analysis because the NIT searches were predicated on facts ostensibly showing that visitors would know its illegal purpose before logging in, given the point in time that the searches could be executed. Nevertheless, this characterization of the site's content is plainly false. It contained, among other things, chat and private message features that allowed visitors to engage in private conversations and the Government understood on February 20,

2015, that these private messages would not necessarily relate to criminal activity.¹¹ This misleading omission (or false statement) implicates substantial First Amendment rights that the Magistrate Judge should have been allowed to consider when determining how much authority to allow the FBI in targeting visitors to the site. *Cf. Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997) (holding that there is “no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]”).

In addition, the affiant was either woefully uninformed or recklessly misleading about how sites are found on the Tor network, going so far as to claim that there is no such thing as a Tor equivalent of a Google search engine. These statements, which make it appear that anyone who found Playpen must be determinedly seeking out child pornography, are simply not true. To the contrary, once someone has downloaded the free Tor browser package that connects them to the network they can explore it with a Tor search engine similar to Google or Bing. *See, e.g.,* <https://ahmia.fi/search>. Using search terms for legal content, such as “sex chat” or “teen erotica,” can readily lead Tor browsers to a variety of sites like Playpen.

These facts, coupled with the absence of any images of “prepubescent” girls or even clear indication that the site contains pornographic pictures (let alone child pornography), are inconsistent with the portrait the affiant was trying to paint of a site that “advertises” itself as “dedicated” to child pornography.

The Government also devoted a substantial portion of the application to describing commonplace features of the site, while at least suggesting that these features were indicative of criminality. For example, the affiant stated that the site “allows users of the TARGET

¹¹ In a separate Title III warrant application also filed on February 20, 2015, (Discovery – Bates 0046) the United States describes how—if the court allowed it to search private chats and messages—the Government would ensure that private chats and private messages that were not criminal in nature would not be further accessed by law enforcement.

WEBSITE to upload links to images of child pornography that are accessible to all registered users of the TARGET WEBSITE.” Ex. B at ¶ 23. This statement is both true and calculated to mislead. The same link and image upload capabilities described by the affiant are basic features of myriad web sites that enable users to post messages and pictures, including everything from pictures of baked goods (*see, e.g.*, epicurious.com) to YouTube videos.

Likewise, the affidavit misleadingly states that the ability of users to exchange names and messages on the site are features “commonly used by subjects engaged in the online sexual exploitation of children.” Ex. B at ¶ 15. These very same features are offered by Twitter and Facebook, among many others. Suggesting that they are in any way indicative of criminality is similar to asserting that bank robbers “commonly” use cars to make a getaway. Millions of innocent people have cars, and the mere fact that someone has a car does not remotely support the conclusion that he or she is likely to be a bank robber.

In sum, the application’s false description of Playpen’s home page, compounded by highly inaccurate statements about how the Tor network functions and a cloud of misleading technical jargon, should persuade the Court that a *Franks* hearing is amply warranted in this case.

C. The NIT Warrant Was Overbroad

The NIT warrant application's probable cause shortcomings are compounded by the extraordinary scale of the search authorization that the Government is claiming. As the Fourth Circuit has recognized, the "Fourth Amendment requires that a warrant be no broader than the probable cause on which it is based." *United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006) (internal quotation marks omitted); *see also United States v. Patrick*, 916 F. Supp. 567, 574 (N.D.W. Va. 1996) ("On its face, the scope of the warrant exceeded the probable cause on which the warrant was based, and it is, therefore, overbroad.").

Here, the Government is advocating an unprecedentedly sweeping exercise of search and seizure powers. Unlike a typical search warrant based upon facts establishing probable cause to search a particular location, the NIT warrant purportedly gave the FBI broad discretion in deciding when and against whom to deploy its malware technology. Specifically, the warrant authorized NIT searches any time someone accessed Playpen's home page, regardless of whether they merely utilized its "chat" forum or their actual activities on the site. *See generally* Kevin Poulsen, *Visit the Wrong Website, and The FBI Could End Up in Your Computer*, Wired.com, August 5, 2014 (although targeted use of "malware" by the FBI is not new, "[w]hat's changed is the way the FBI uses its malware capability, deploying it as a driftnet instead of a fishing line").¹²

As a result, the NIT warrant may fairly be characterized as the Internet age equivalent of a general warrant, allowing the FBI to search tens of thousands of computers for which probable cause to search was not established. Worse yet, as noted above, the warrant could easily have been narrowed to authorize searches of only those site visitors who viewed or downloaded illegal

¹² Available at http://www.wired.com/2014/08/operation_torpedo/ (last accessed Mar 16, 2016).

pornography, an appropriately circumscribed line to draw given that illicit content was contained in specific sub-directories on the site. Since the FBI could send its malware to anyone who logged into the site, the warrant could simply have required the FBI to target only those people who “clicked” on particular sub-directories with illegal content or particular pictures or links in those sub-directories. Indeed, in a footnote, *the affiant acknowledges that the FBI could do exactly that*, yet the warrant does nothing to particularize or narrow the set of visitors who would be subjected to searches. Ex. B at ¶ 32, n. 8.

In a recent case, a district judge applied the common sense principle that applies here in a more traditional setting:

[W]hen, as in this case, a warrant’s scope is so broad as to encompass “any and all vehicles” at a scene, without naming any vehicle in particular, the probable cause on which it stands must be equally broad. Specifically, the Fourth Amendment requires that the probable cause showing in support of an “any and all vehicles” warrant must demonstrate that, at the time of the search, a vehicle’s mere presence at the target location is sufficient to suggest that it contains contraband or evidence of a crime.

United States v. Swift, 720 F. Supp. 2d 1048, 1055-56 (E.D. Ark. 2010). Here, the Government perhaps could have requested a warrant with a narrower scope. Instead the Government chose to go for breadth. Yet a broad warrant is valid only when the probable cause showing is equally broad. Here—like the mere presence of a car at the scene of a crime—the Government sought to search users’ computers based on mere entry to the Playpen site even though it was not clear from the homepage that someone merely entering the Playpen site—perhaps for the first time—intended to access child pornography.

Courts have recognized that “over-seizing is an inherent part of the electronic search process” and have noted that this “calls for greater vigilance on the part of judicial officers” when it comes to computer searches. *United States v. Comprehensive Drug Testing, Inc.*, 621

F.3d 1162, 1177 (9th Cir. 2010). The Fourth Amendment's specificity requirements were designed "to prevent a general, exploratory rummaging." *United States v. Oloyede*, 982 F.2d 133, 138 (4th Cir. 1992) (internal quotation marks omitted). Hence, "[a] warrant must not only give clear instructions to a search team, it must also give legal, that is, not overbroad, instructions." *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702-03 (9th Cir. 2009), quoting *In re Grand Jury Subpoenas*, 926 F.2d 847, 857 (9th Cir. 1991); see also *United States v. Talley*, 449 F. App'x 301, 302 (4th Cir. 2011) ("The requirement for particularity ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.") (internal quotation marks omitted). Nevertheless, in this case, the FBI sought the broadest possible search authorization, encompassing many thousands of targets, and the warrant itself did nothing to narrow or focus that authorization.

In short, the NIT warrant implicates the Fourth Amendment's core purpose of guarding against overbroad and unreasonable searches for several reasons. It allegedly authorized the FBI to execute searches on a population of potential targets so large that it exceeds the population of Charlottesville, Virginia, and many other small cities. If the Government is correct, the warrant granted this unprecedented search and seizure authority based on a showing of probable cause that, even taking the facts in the warrant application at face value, was insufficient. With the *Franks* violations taken into consideration, the overbreadth of the warrant is even more striking and, standing alone, warrants suppression.

D. The NIT Warrant was an Anticipatory Warrant and, Regardless of the False and Misleading Statements in the Supporting Affidavit, the "Triggering Event" for the Computer Searches Failed.

The NIT warrant was an anticipatory warrant because it prospectively authorized searches whenever unidentified Playpen visitors signed on to the site, with the "triggering event"

for those searches being the act of accessing the site. *See* ex. B at ¶ 32 (requesting authority “to use the NIT. . . to investigate any user or administrator *who logs into* the TARGET WEBSITE by entering a user name and password”) (emphasis added). As the Supreme Court has explained, the execution of an anticipatory search warrant is subject “to some condition precedent” that actually gives rise to the probable cause; this is generally referred to as a “triggering condition.” *United States v. Grubbs*, 547 U.S. 90, 94 (2006). It is axiomatic that “[i]f the triggering event does not occur, probable cause to search is lacking.” *United States v. Vesikuru*, 314 F.3d 1116, 1119 (9th Cir. 2002); *see also United States v. Rowland*, 145 F.3d 1194, 1201 (10th Cir. 1998) (“If the triggering events do not occur, the anticipatory warrant is void.”); *cf. United States v. Turner*, 491 F. Supp. 2d 556, 560 (E.D. Va. 2007) (suggesting that search is invalid if “triggering condition never occurred”).

In this case, there was probable cause to search the computers of everyone who signed into Playpen (the triggering event) only if the site continued to “unabashedly announce” that it was dedicated to child pornography. *Martin*, 426 F.3d at 75. Assuming, for the sake of argument, that the warrant application’s description of pornographic pictures on the home page had established probable cause to believe that anyone who entered the site was a legitimate search target, the foundation for that conclusion was undermined when that description proved to be inaccurate.

Without illegal images on the public home page, all that remains to establish probable cause is the technical verbiage on the home page, which is not indicative of illegal activity; general and erroneous assertions about how sites can be found on the Tor network; and the allegations about the site’s content. The content, moreover, is largely irrelevant because the warrant authorized searches before users could even see that content.

The home page—as it actually appeared when the warrant was approved and the searches were executed—contains little, if anything, that would lead an unwitting visitor to believe that Playpen was more than a common pornography site or sexually oriented chat room. As a result, ***the triggering event as established in the warrant application could not, and did not, occur.*** Since the triggering event could not occur, searches based on the NIT warrant inevitably exceeded the scope of its authorization.

Nevertheless, without alerting the Virginia court to its errors or submitting a revised warrant application, the Government proceeded to search the computers of site visitors for at least two more weeks as if nothing had changed. Regardless of whether this sequence of events was the result of intentional or reckless conduct, or is attributable to mere carelessness, key facts that the Government had relied on to establish probable cause and the triggering event for the searches no longer existed by the time those searches were executed. Consequently, when the Government proceeded with the NIT searches anyway, it was acting outside the scope of the warrant, and suppression is required. *See Vesikuru*, 314 F.3d at 1123 (if the “triggering events did not occur, the warrant was void, and evidence gathered from the search would have to be suppressed.”).

CONCLUSION

The search of Mr. Darby’s home computer was undertaken as part of an unprecedentedly sweeping and dragnet search and seizure operation that targeted 100,000 or more private computers throughout the United States and elsewhere. The warrant application that the Government has relied on for these searches did not establish probable cause, and in fact the FBI made false statements and withheld information from the issuing judge that was material to determining probable cause.

Moreover, even if probable cause had been anticipated assuming some future occurrence—the “triggering event”—that necessary antecedent for probable cause never occurred. Accordingly, the Court should suppress all evidence seized during the January, 2016, search of Mr. Darby’s home computer and all fruits of that search.

Respectfully submitted,

GERALD A. DARBY

By: _____/s/_____

Rodolfo Cejas, II
VSB # 27996
Assistant Federal Public Defender
Attorney for Gerald A. Darby
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0800
(757) 457-0880 (telefax)
rodolfo_cejas@fd.org

CERTIFICATE OF SERVICE

I certify that on the 13th day of April, 2016, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following:

Elizabeth Yusi, Esquire
United States Attorney's Office
101 West Main, Suite 8000
Norfolk, Virginia 23510
(757) 441-6331
Email: elizabeth.yusi@usdoj.gov

By: _____/s/ _____

Rodolfo Cejas, II
VSB # 27996
Assistant Federal Public Defender
Attorney for Gerald A. Darby
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0800
(757) 457-0880 (telefax)
rodolfo_cejas@fd.org